REMARKS

The Office Action dated November 10, 2004 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto.

Claims 1-21 stand rejected and pending and under consideration.

REJECTION UNDER 35 U.S.C. § 103:

In the Office Action, at page 2, claims 1, 2, 14, and 15 were rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,751,812 to Anderson ("Anderson") and U.S. Patent No. 5,862,225 to Feldman et al. ("Feldman"). The Office Action took the position that Anderson and Feldman disclose all the aspects of claims 1, 2, 14, and 15. The rejection is traversed and reconsideration is requested.

Independent claim 1, upon which claims 2-13 are dependent, recites a method for user identification and ascertainment of authenticity of parties in a telecommunication system comprising: a telecommunication network, a source system connected to the telecommunication network, a target system connected to the telecommunication network, said method comprising the steps of: storing user identifiers and associated passwords in the source system and in the target system, logging on into the source system by entering a user identifier and a password corresponding to it, identifying the user in the source system, setting up a remote session to the target system, The method further comprises the steps of: generating identical indexed encryption keys in the source system and in the target system, encrypting the password associated with the user

identifier in the source system using the encryption key indicated by a first index, and sending the encrypted data as well as the first index and the user identifier to the target system, encrypting the password associated with the user identifier in the target system using an encryption key indicated by the index received, performing a first comparison between the received password and the password encrypted in the target system, encrypting in the target system the password received from the source system using an encryption key indicated by a second index, and sending the encrypted data and the second index to the source system. The method further comprises the steps of encrypting the encrypted password initially sent from the source system to the target system again using the encryption key indicated by the second index received from the target system, performing a second comparison between the encrypted password received from the target system and the password encrypted in the source system using the encryption keys indicated by the first and second indexes, and approving the setup of the remote session if the results of the comparisons are coincident.

Independent claim 14, upon 15-21 are dependent, recites a system for user identification and ascertainment of authenticity of parties in a telecommunication system comprising: a telecommunication network, a source system connected to the telecommunication network, a target system connected to the telecommunication network. In the system, it is possible to store user identifiers and associated passwords in the source system and in the target system, log on into the source system by entering a user identifier and a password corresponding to it, identify the user in the source system

and set up a remote session to the target system. The system comprises: means for generating identical indexed encryption keys in the source system and in the target system, means for encrypting data in the source and target systems using an encryption key indicated by an index, means for transmitting data between the source and target systems, means for performing a comparison in the source and target systems, and means for approving the setup of a remote session.

As will be discussed below, the cited prior art of Anderson and Feldman fail to disclose or suggest the elements of any of the presently pending claims.

Referring to Anderson, this reference generally provides secure password systems which utilize iterated hash functions and therefore require periodic re-initialization. See column 1, lines 6-12. Anderson only allows comparing two hash values that have been calculated with two subsequent index values *i*. See column 2, lines 1-16. That is, if the server receives a hash value $H^{i-1}(A)$ calculated using a first index value *i-1*, the server can only compare the presently received hash value with a previously received has value $H^{i}(A)=H(H^{i-1}(A))$ calculated using a preceding index value *i*. The very nature of the S/Key™ system employed by Anderson requires the index values to be subsequent to each other, e.g., *i* and *i-1*, in order to enable the comparison.

In contrast, according to an aspect of the present invention, independent claim 1 recites, in part, "encrypting the password associated with the user identifier in the source system using the encryption key indicated by a first index, and ... encrypting the encrypted password initially sent from the source system to the target system again using

the encryption key indicated by the second index received from the target system." The first index recited in independent claim 1, as indicated in the Office Action, is the hash value $H^{i-1}(A)$ of Anderson. Also, the second index recited in independent claim 2, as indicated in the Office Action, is value $H^{i}(A)=H(H^{i-1}(A))$ calculated in Anderson. Values thus obtained from the recitations of independent claim 1 are then compared. Yet, the only comparison allowed by Anderson is $H^{i}(A)=H(H^{i-1}(A))$, in which two subsequent index values *i* have been employed.

The Office Action correctly recognized that Anderson fails to teach or suggest all the recitations of independent claim 1 including encrypting in the target system the password received from the source system, encrypting the encrypted password, performing a second comparison , and approving the setup of the remote session. Accordingly, the Office Action relied on Feldman as providing for such recitations.

Feldman generally describes a system for resynchronizing a receiver with a transmitter if the receiver and the transmitter are asynchronized. See column 2, lines 26-47. The system of Feldman includes a first memory device for storing an old encrypted message, as well as a second memory device for storing a new encrypted message transmitted by the transmitter and received by the receiver. However, Feldman is silent as to teaching or suggesting, at least, "encrypting in the target system the password received from the source system using an encryption key indicated by a second index," as recited in part in independent claim 1. There is no teaching or suggestion in Feldman that either the old encrypted message or the new encrypted message is encrypted using an

encryption key indicated by a second index. Although Feldman generally provides re-encrypting the old encrypted message and testing whether the re-encrypted old message matches the new message, Feldman does not teach or suggest that the re-encryption of the old encrypted message is performed "using the encryption key indicated by the second index received from the target system," as recited in part in independent claim 1.

In addition, in Feldman, if the new message matches the re-encrypted old message, the microcomputer decrypts the new message and initiates a command within the decrypted new message. If the new message in Feldman does not match the re-encrypted old message, the microcomputer re-encrypts the re-encrypted old message, and decrements a counter each time the re-encrypted old message is re-encrypted. However, nothing in Feldman provides that the matching is performed "using the encryption key indicated by the first and second indexes," as recited in part in independent claim 1. Rather, in Feldman, where a match is made, the new message is decrypted and the command within the decrypted new message is initiated by the microcomputer. Therefore, Applicant respectfully submits that Feldman does not cure the deficiencies of Anderson as discussed above with regard to independent claims 1 and 14.

Furthermore, as commonly understood, the U.S. Patent Office bears the burden of establishing a prima facie case of obviousness based upon the prior art..."[the U.S. Patent Office] can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references." See In re Fritch, 23

USPQ 2d 1780, 1783 (Fed. Cir. 1992). In addition, the mere fact that the prior art may be modified in the manner suggested by the Office Action does not make the modification obvious unless the prior art suggested the desirability of the modification. Id. at 1783-84. Rather than providing some objective teaching in the references cited, conclusive statements are made such as "it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Feldman et al within the system of Anderson so as to ensure a secure log-in by a user to a network. Re-encrypting the hash function is a repetition of the initial encryption of the hash function, which is already known in the art as a form of message authentication."

However, Anderson generally describes an S/Key™ system utilizing a hash function H that can be iterated, whereas Feldman describes an encryption scheme calculating rolling codes. The two encryption schemes appear to be completely different, and there is nothing in Anderson or Feldman to suggest that both references may be combined.

"Rejection of patent application for obviousness under 35 USC §103 must be based on evidence comprehended by language of that section, and search for and analysis of prior art includes evidence relevant to finding of whether there is teaching, motivation, or suggestion to select and combine references relied on as evidence of obviousness; factual inquiry whether to combine references must be thorough and searching, based on objective evidence of record." See In re Lee, 61 USPQ2d 1430 (CA FC 2002).

Thus, as pointed out in In re Lee, the record must support motivation, i.e., there must be something in the record pointing out where the recited motivation can be found. In addition, there must be some discussion on how that purported motivation or suggestion is even relevant to the reference being modified.

Only the present invention sets forth all the claimed features, as well as the motivation for combining the same. The outstanding rejection would appear to have taken this teaching of the present invention and applied the same to generate a combination of Anderson and Feldman, as set forth in the Office Action, to disclose the presently claimed invention. Applicant respectfully asserts that the prima facie burden has not been met and the obviousness rejection fails.

Because independent claim 14 includes similar claim features as those recited in independent claim 1, although of different scope, and because the Office Action refers to similar portions of the cited references to reject independent claim 14, the arguments presented above supporting the patentability of independent claim 1 are incorporated herein to support the patentability of independent claim 14.

Therefore, Applicant respectfully asserts that the rejection under 35 U.S.C. §103(a) should be withdrawn because neither Anderson nor Feldman, whether taken singly or combined, teaches or suggests each feature of independent claims 1 and 14 and hence, dependent claims 2-13 and 15-21.

In the Office Action, at page 4, claims 3-13 and 16-21 were rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,751,812 to Anderson ("Anderson"), U.S. Patent No. 5,862,225 to Feldman et al. ("Feldman"), and further in view of U.S. Patent No. 5,784,464 to Akiyama et al. ("Akiyama"). The Office Action took the position that Anderson, Feldman, and Akiyama disclose all the aspects of claims 3-31 and 16-21. The rejection is traversed and reconsideration is requested.

As will be discussed below, the cited references of Anderson, Feldman, and Akiyama fail to disclose or suggest the elements of any of the presently pending claims.

Dependent claims 3-13 depend upon claim 1 and thereby inherit all of the patentable distinctions thereof. Dependent claims 15-21 depend upon claim 14 and thereby inherit all of the patentable distinctions thereof. Therefore, Applicant respectfully submits that claims 3-13 and 15-21 are patentable over Anderson and Feldman at least for the reasons discussed above in connection with independent claims 1 and 14.

Akiyama generally describes a first encrypting element encrypting a random number with the first key outputted by the key outputting unit, thereby outputting the first authenticator. See column 4, lines 11-37. On the other hand, when a second receiving element of the client receives the random number, a second encrypting element encrypts this random number with the second key identical with the first key held by the key holding element, thereby outputting the second authenticator. The second transmitting element transmits the second authenticator to a data supplying apparatus.

In addition, in Akiyama, when the first receiving element of the data supplying apparatus of Akiyama receives the second authenticator, the comparing element compares the first authenticator with the second authenticator and, if the two authenticators are the same, authenticates the access request given from the relevant client. However, Akiyama does not cure the deficiencies of Anderson and Feldman. Similarly to Anderson and Feldman, Akiyama does not teach or suggest, at least, "encrypting the encrypted password initially sent from the source system to the target system again using the encryption key indicated by the second index received from the target system;...performing a second comparison between the encrypted password received from the target system and the password encrypted in the source system using the encryption keys indicated by the first and second indexes," as recited in independent claim 1. Anderson does not provide encrypting again an encrypted password initially sent from the first transmitting element to the second transmitting element. Furthermore, Anderson does not teach or suggest that that the comparing element uses the first and second keys to compare an encrypted first authenticator with an encrypted second authenticator.

Also, similarly to Anderson and Feldman, Akiyama does not teach or suggest, "performing a second comparison between the encrypted password received from the target system and the password encrypted in the source system using the encryption keys indicated by the first and second indexes," as recited in independent claim 1. Instead, in

Akiyama, a comparison alone is made between the first authenticator with the second authenticator.

Furthermore, Applicant respectfully submits that the Office Action has pieced together three references to teach the claimed invention. However, MPEP 2143.01 instructs that "[t]he mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination." See In re Mills, 916 F.2d 680, 16 USPQ 2d 1430 (Fed. Cir. 1990). MPEP 2143.01 further instructs that "[a]lthough a prior art device 'may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so.'" Applicant respectfully submits that the cited references do not provide such a suggestion or motivation. Applicant submits that the only motivation to piece together the three references of the Office Action is found in Applicant's own application.

Thus, even if Anderson, Feldman, and Akiyama were combined, a combination thereof would fail to teach or suggest all the recitations of independent claim 1. For similar reasons, the combination of the cited references would also fail to teach or suggest all the recitations of independent claim 14. It is respectfully requested that independent claims 1 and 14 and related dependent claims 3-13 and 16-21 be allowed.

CONCLUSION:

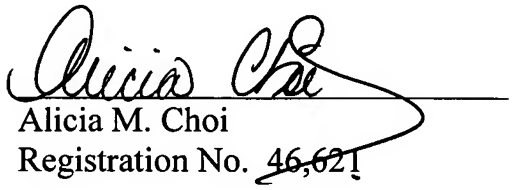
In view of the above, Applicant respectfully submits that the claimed invention recites subject matter which is neither disclosed nor suggested in the cited prior art. Applicant further submits that the subject matter is more than sufficient to render the claimed invention unobvious to a person of skill in the art. Applicant therefore respectfully requests that each of claims 1-21 be found allowable and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicant respectfully petitions for an appropriate extension of time.

Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Alicia M. Choi
Registration No. 46,621

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

AMC:jf